

## e2Campus Insight—Text Messages and SMPP vs. SMTP

When considering an Emergency Notification System (ENS) the speed at which messages can be delivered to your users is an important factor. In order to understand how fast a message can reach your community, it is vital to know the differences between the technologies used to transmit SMS messages. Your vendor transmits SMS text messages on your behalf. In this issue of e2Campus Insight, we will talk about the different SMS messaging protocols and how they can affect SMS text message delivery.



### What Is SMS?

**Short Message Service (SMS)** is the text communication service component of phone, web or mobile communication systems, using standardized communications protocols that allow the exchange of text messages between fixed line or mobile phone devices. SMS text messaging is the most widely used data application in the world, with 2.4 billion active users, or 74% of all mobile phone subscribers. The term SMS is used as a synonym for all types of short text messaging as well as the user activity itself in many parts of the world. When we refer to SMS Messaging, we're talking about text messaging, as it pertains to your users mobile phones.

Cell phone carriers classify SMS messages into two types: Mobile Originated messages and **Mobile Terminated** messages. **Mobile Originated** messages are messages that have been sent by a mobile phone subscriber, usually to another mobile phone. Most subscribers simply consider this 'text messaging'. A Mobile Terminated message is a message that is destined to be delivered to a mobile phone subscriber, but originates elsewhere, such as from a service like E2Campus.

There are two major methods for sending SMS messages in the United States:

- **SMPP** – Short Message Peer-to-Peer Protocol
- **SMTP** - Simple Mail Transfer Protocol

### SMPP

SMPP is a telecommunications protocol used specifically to exchange SMS messages between cell phone carriers, as well as external entities such as Emergency Services like e2Campus, voting systems that process SMS votes, or other web-to-mobile or mobile-to-web products. SMPP is designed to be fast and efficient to facilitate high volume reliable message exchange. SMPP messages are sent via "Common Short Codes". Short codes are short-form phone numbers used for mass texting. Carriers each contract with gateway providers, called "aggregators" who maintain dedicated, secure connections with the carriers and route SMS sent using registered short codes.

In order to register and use a short code, a sender must engage in a lengthy provisioning process. This process involves extensive verification of the sending application's purpose, processes and usage. The aim of the provisioning process is to ensure that the sender is legitimate and will follow the rules set forth by the carriers. As such, this serves as a barrier to entry for companies desiring to enter the ENS marketplace, as the provisioning process is time consuming and expensive. Additionally, each message sent through a short code bears a small cost to the sender. Any ENS sending via short code (SMPP) must pay for the texts sent. This also serves a barrier to entry for many companies entering the ENS market. However, this cost comes with benefits, such as increased throughput, reliability, and reporting capabilities.

SMPP also provides the capability of two-way communication. The recipient can respond to SMS sent through a short code to opt-in, and, importantly, opt-out of messages. The sender must obey basic text commands, such as "STOP" and "HELP". This ensures that recipients of short code text can control what texts reach their phone and receive instructions on how to get technical assistance with any short code service.

- **Reliability:**

Since SMPP uses dedicated aggregators to send bulk SMS, the reliability rate for delivery is very high. Delivery success rates of 95% or higher are not uncommon with registered (Opt-In) messages sent via SMPP. Each message is routed by the aggregator through a registered short code that is pre-provisioned with the carriers. This ensures that messages should not be filtered or blocked as "spam".

Aggregators also maintain SMS routing information provided by all carriers that they support. This means that messages will route to recipients, even if they should switch carriers, as long as the new carrier is also capable of receiving SMPP (short code) text messages.

SMPP (short code) texting also provides message delivery tracking, so the sender can tell if the message was accepted by the recipient's carrier. Some carriers have also added additional delivery tracking, allowing the short code sender to track delivery to the recipient's handset. This helps ensure reliability in that the sender can quickly identify delivery problems that may otherwise go undetected.

- **Speed:**

SMPP is designed specifically for large-scale bulk messaging. As such, message transmission is very fast. Transmission speeds of

### e2Campus and SMS

e2Campus uses a combination of SMPP and SMTP messaging. When a carrier supports SMPP messaging, Amerliert sends its SMS messages via high-volume SMPP—as fast as 18,000 SMS text messages every minute. We also retain individual relationships with carriers that do not support SMPP, and send messages to them via their dedicated SMTP connections.

e2Campus SMS notifications reach subscribers even if wired and wireless networks are jammed with callers. During a crisis when voice and data networks are all jammed, the small size of a SMS text message alert often goes through first.

When sending an alert the differences between SMS messages that are sent via SMPP vs. SMTP are important to keep in mind. It is imperative to understand the issues discussed in this paper and ask your ENS vendor which protocols they use to transmit SMS alerts.

18,000 texts per minute are common. Since all short codes are pre-approved by carriers, spam blocking is not a concern. Carriers have already cleared the sender for bulk messaging and should not ever “spam block” texts from short codes.



- **Security:**  
All SMPP based text messages are sent through registered short codes. Since all SMPP connections use securely encrypted, dedicated connections, SMPP is the most secure method for sending SMS. “Spoofing” a short code is not a simple task as one would need to hack into the aggregator itself in order to send a hoaxed short code.

## SMTP

SMTP is a protocol that is used for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another. In addition, SMTP is sometimes offered by Cell Phone Carriers as an option for SMS text messaging so that messages can be sent from SMTP servers to mobile phones.



- **Reliability:**  
Since this method of transmission uses the same protocol as e-mail, sending SMS via SMTP is subject to the same pitfalls and delays that any e-mail message will encounter.. Messages sent can easily be filtered as “spam”, especially when a carrier receives high volumes of traffic with the same message. Carriers are in a constant battle against e-mail spam and thus delays and blockage can and should be expected when sending SMS via SMTP.  
  
The nature of SMTP, being an open method for sending e-mail, can also lead to confusion regarding its use and the CAN-SPAM Act (<http://www.fcc.gov/cgb/consumerfacts/canspam.html>) and thus many carriers are quick to block SMS sent through this method. SMTP must be routed directly to the subscriber’s carrier, typically by formatting the message as “<number>@<carrier\_domain\_name>”. If a subscriber changes carriers, that subscriber must update the subscription or future messages will not be delivered. There is no chance of a message routing to the new carrier as is commonly seen with short code texting.  
  
SMTP also provides no real delivery reporting, so you’re often not sure if the message was received by the end user at all.
- **Speed:**  
Sending SMS via SMTP is typically slower than SMPP, as the message is routed through the public switched internet, just like any e-mail message. As such, text may bounce through any number of servers before reaching the carrier. At that point, it must pass through the carrier’s e-mail spam filter/firewall and on to the recipient. As such, the quality of service for SMS via SMTP is equivalent to any e-mail message.
- **Security:**  
Spoofing an e-mail address is not difficult. A quick search on Google for “how to spoof an email address” will net you about 1.4 million hits, including several YouTube videos showing anyone how to fake a sender address in seconds.  
  
Since the SMS standard does not allow you to see the detailed headers of the sender of an e-mail message, the recipient has no way to tell a fake from the real thing when it comes to SMS via SMTP.  
  
If you’re at all concerned about hoaxes, SMS via SMTP should be avoided whenever possible.

## Why use SMTP at all?

While SMTP has reliability issues, is slower than SMPP and can have some security concerns, many small regional and pre-paid cell phone carriers only support SMTP messaging.

The benefit for many ENS companies is that the cost of sending text messages through SMTP is much lower when compared to SMPP. Since short code (SMPP) texts carry a cost per-message and e-mail is essentially free, there is a financial incentive for ENS companies to try to use SMTP.

## What This Means for You

A primary advantage of using SMPP for SMS is that the user’s mobile device often receives message notifications **much faster** than when using SMTP. There are also many other advantages of using SMPP over SMTP. Messages through SMPP are **secured, reliable in delivery, and carrier supported**, unlike SMTP. SMPP is a direct connection to carriers and provides **instant delivery**, while SMTP messages do have higher rate of delivery failure. Messages sent via SMTP roam around the Internet from server to server with all the other regular internet traffic before they get delivered. If there is internet congestion, or if servers are fully loaded, much like e-mail, SMS via SMTP can take hours to get delivered—time that is important when issuing a possible life-saving alert message.



e2Campus by OMNILERT, LLC  
525-K East Market Street, # 232  
Leesburg, Virginia 20176  
800-936-3525

[www.e2Campus.com](http://www.e2Campus.com)  
[info@e2Campus.com](mailto:info@e2Campus.com)